IN THE SPECIFICATION:

On page 4, line 14:

As shown in FIGURE 2, a user using a user system 28 creates or retrieves an electronic document that they wish to designate for review and signing by others, see block 80. An example of electronic documents are parseable documents, such as those created in word processing programs (e.g. MS Word, Adobe Reader, etc.). Next, at block 82, the user identifies one or more blocks of text requiring review by others. An example of identifying a block of text is described in FIGURE 4 below. At block 83, one or more tag data structures are created for each identified block of text and associated with the document the text is from. Tag data structure creation is described by example in FIGURE 4. At block 84, the document with the identified one or more blocks of text is sent by the user to the digital signature server 22 via the network 30 for uploading and processing, thereby registering the document, see FIGURE 9. At block 86, the digital signature server 22 finds the identified blocks of text within the document according to the created tag data structures that are associated with the document. The digital signature server 22 or a processing component thereof analyzes a registered document for associated created tag data structures and/or message digests. Then, at block 88, the user interacting with a user interface, described below in FIGURE 10, assigns tasks for others to perform on the document or on a the found blocks of text within the document. Once the user has completed the assignment of tasks, the digital signature server 22 makes the document available to those users that have been assigned tasks, see block 90.

On page 5, line 1:

FIGURE 3 illustrates a method a user performs in order to complete tasks assigned to them for documents registered with the digital signature server 22. First, at block 100 the user connects to the digital signature server 22. In one aspect embodiment of the present invention the connection is a connection over the Internet and requires that the user using a user system 28

BLACK LOWE & GRAHAM PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

logs onto a web site hosted by the digital signature server 22. In one embodiment, the user has preregistered with the server 22 and has received a password required for later logons. Next, at block 102, the user receives notification of documents with assigned tasks not yet before. In one embodiment, a user interface or web page identifies a list of documents requiring tasks to be performed by that user. Various other information is associated with assigned tasks, such as deadline dates, others required to review and sign documents history information. Then, at block 103, the user selects a document with assigned task or tasks not yet performed. At decision block 104, if a task requiring the user to perform is not a signing task, the digital signature server 22 will request that the user perform the desired task. However, if an assigned task is a signing task, then, at block 106, the user reviews any identified blocks of text requiring action. At block 108, the user selects an option associated with each of the identified blocks of text within the document. At decision block 110, if there remain ~~remains~~ options associated with identified blocks of text with in the document that have not been completed, the process returns to block 106 until the user completes the selection of the options associated with all the identified blocks of text. Once the user has completed the selection of all options associated with all the identified blocks of text, then, at block 112, the electronic signing of the document is performed. FIGURE 10 shows example web page a user might see when reviewing for the purpose of applying a digital signature.

On page 8, line 1:

Standards for digital signature are defined within the Public-Key Cryptography Standards (PKCS). Public-key cryptography is an asymmetric cryptography technology. In asymmetric encryption and decryption, two keys are used. Data encrypted with ~~the~~ either key may be decrypted by using the other. Typically, the value of one key is kept secure (generally referred to as the private key), while the second keys value is widely shared (the public key). Digital signature technology exploits this implementation.

BLACK LOWE & GRAHAM PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301